https://doi.org/10.37528/FTTE/9788673954455/POSTEL.2021.009

BLOKČEJN - SIMULACIONO TESTIRANJE MREŽE I REALIZACIJA PAMETNOG UGOVORA JAVNE PRODAJE

Marko Đogatović, Nikola Matijašević,
Univerzitet u Beogradu - Saobraćajni fakultet,
m.djogatovic@sf.bg.ac.rs, nikola.matijasevic@sf.bg.ac.rs

Rezime: *Iako su stvorena različita rešenja zasnovana na blokčejn tehnologiji, nedostatak alata za procenu ovih složenih distribuiranih sistema može ometati razvoj i napredak ove oblasti. Istraživanje različitih implementacija i različitih varijacija projektovanja blokčejn mreža je složeno i teško izvodljivo na realnim sistemima. Sa druge strane, blokčejn simulatori daju mogućnost praćenja procesa u mreži uz niske troškove. Simulatori mogu testirati performanse mreže koristeći različita podešavanja na jednom računaru. Ovaj rad pruža analizu 7 blokčejn simulatora i njihovo poređenje. Takođe, blokčejn tehnologija je korišćena za realizaciju procesa javne prodaje (aukcije) sadržine neisporučivih poštanskih pošiljaka. Ovaj proces se realizuje na blokčejnu korišćenjem pametnih ugovora.*

Ključne reči: *blokčejn, Bitcoin, blokčejn simulator, pametan ugovor, javna prodaja.*

1. Uvod

Krajem 2008. godine, objavljen je rad gde je opisana *peer-to-peer* (P2P) verzija elektronskog novca (kriptovalute), pod imenom *Bitcoin*, koji omogućava plaćanje bez posredovanja finansijskih institucija [1]. *Bitcoin* je digitalni novac pomoću kojeg se vrše transakcije putem Interneta u decentralizovanoj nepouzdanoj mreži korišćenjem javne baze podataka koja se naziva blokčejn. Danas se blokčejn tehnologija primenjuje na širokom polju različitih rešenja izvan kriptovaluta. Međutim, decentralizovana priroda blokčejna ograničava performanse što postaje ograničenje za širu primenu ove tehnologije.

Složenost velikih blokčejn mreža čini proces procene performansi izazovnim. Generalno, izvođenje eksperimenata na blokčejnu je skupo i komplikovano. Zbog toga, simulacija blokčejn mreža postaje prikladan pristup za procenu performansi. Blokčejn simulatori daju mogućnosti testiranja procesa u mreži uz male troškove. Oni imaju za cilj da reprodukuju performanse i funkcionalnosti stvarne mreže tokom vremena primenom i pokretanjem simulacionog modela.

Posebnu funkcionalnost *Ethereum* platforme predstavljaju pametni ugovori. Oni se definišu kao kompjuterizovani protokoli za transakcije koji izvršava uslove ugovora [2]. Ciljevi pametnog ugovora su da se zadovolje zajednički uslovi ugovora, da se minimiziraju zlonamerne ili slučajne pojave i da se minimizira potreba za pouzdanim posrednicima.

Ostatak rada je organizovan na sledeći način. U drugom poglavlju, objašnjavaju se tipovi blokčejn mreža, šta čini njenu strukturu, grupe konsenzus protokola i princip rada. Cilj trećeg poglavlja je da izvrši poređenje blokčejn simulatora prema karakteristikama i prema ulaznim i izlaznim parametrima. Četvrto poglavlje prolazi kroz proces obavljanja javne prodaje sadržine neisporučivih poštanskih pošiljaka i njegovu realizaciju na blokčejnu pomoću pametnog ugovora. U petom poglavlju su data zaključna razmatranja.

2. Blokčejn tehnologija

Blokčejn tehnologija predstavlja decentralizovanu i distribuiranu bazu podataka koja ima za cilj evidentiranje svih transakcija koje su se ikada dogodile u mreži. Cilj takve baze podataka je stvaranje nepromenljivog zapisa svih transakcija i njihove vidljivosti za svakoga ko prati ili koristi blokčejn. U ovom poglavlju biće predstavljeni tipovi, struktura, konsenzus protokoli i princip rada blokčejn tehnologije.

2.1. Tipovi blokčejn tehnologije

Blokčejn mreže se dele, u skladu sa njenom otvorenošću pristupa, na javni i privatni blokčejn [3]. U skladu sa tim da li se radi o javnoj ili privatnoj blokčejn mreži, može doći do određenih promena u ostalim segmentima tehnologije.

Bitcoin, kao prva i najpoznatija platforma blokčejn tehnologije, javlja se kao glavni predstavnik javnog tipa. Glavna karakteristika ovog tipa jeste da između čvorova ne postoji poverenje i da njihovi identiteti nisu poznati [3]. Takođe, svako može da pristupi mreži (ili da je napusti) i da dodaje blokove u lanac ukoliko ima pristup Internetu.

Glavni predstavnik privatnog tipa jeste platforma *Hyperledger*. Privatne blokčejn platforme su one gde čvorovi moraju biti autentifikovani i autorizovani od strane nekog autoriteta [3]. Usled toga što samo autorizovani čvorovi održavaju mrežu, moguće je ograničiti ko može da čita istoriju transakcija i ko može da izvršava transakcije. Čvorovi između sebe imaju određeni nivo poverenja jer su oni autorizovani da dodaju blokove i ukoliko počnu da se ponašaju zlonamerno, njihova autorizacija može biti povučena.

2.2. Struktura blokčejn tehnologije

Blokčejn je struktura koja se sastoji od blokova i koji su međusobno povezani lancem. Lanac blokova ne postoji u realnom svetu, već u digitalnom. Suština postojanja blokova jeste da skladište transakcije koje su se desile u mreži, dok se lanac odnosi na kriptografsku heš funkciju koja povezuje ove blokove i čini vezu „neraskidivom“. Jedan blok se sastoji od spoljašnjeg zaglavlja, zaglavlja i tela bloka [4]. Spoljašnje zaglavlje bloka identifikuje blokčejn platformu i govori o veličini bloka (maksimalni broj bajtova u bloku). Najbitniji deo je zaglavlje bloka jer sadrži informacije o validaciji bloka i podatke o prethodnom bloku. Telo bloka se sastoji od brojača i liste transakcija.

Zaglavlje bloka svake blokčejn platforme treba da sadrži verziju bloka, heš roditeljskog bloka, jednokratni broj, vremenski žig, koren Merkle stabla i cilj heša [4]. U procesu dodavanja bloka u lanac najbitniji su heš roditeljskog bloka (rezultat heš funkcije sa zaglavljem prethodnog bloka kao ulaz), jednokratni broj (menja se kroz iteracije) i cilj heša (fiksirana heš vrednost u mreži).

2.3. Konsenzus protokoli blokčejn tehnologije

Ključni deo je određivanje čvora koji dodaje sledeći blok u lanac. Kako čvor ne zna prave identitete drugih čvorova u mreži, sledi da ne može imati potpuno poverenje u njih. Konsenzus protokoli služe za zamenu poverenja između čvorova kako bi se omogućio grupni rad i ostvario zajednički cilj [5]. Dve glavne grupe konsenzus protokola su [3] [4]: *Proof-of-X* (PoX) i *Byzantine Fault Tolerant* (BFT) algoritmi.

PoX algoritmi se primenjuju za javne tipove blokčejn mreža i koriste računarske proračune kako bi se na slučajan način izabrao čvor koji dodaje sledeći blok u lanac. Glavni predstavnik ove grupe je *Proof-of-Work* (PoW) algoritam. U njemu čvor stiče pravo da objavi sledeći blok kroz takmičenje sa drugim čvorovima u rešavanju kriptografskog problema. Kod rešavanja ovog problema, potrebno je posvetiti pažnju jednokratnom broju i cilju heša. Kako je cilj heša fiksiran, potrebno je uticati na jednokratni broj kako bi se došlo do rešenja. On se povećava kroz iteracije i izračunava se nov heš zaglavlja bloka kako bi se uporedio sa ciljem heša. Kriptografski problem se smatra rešenim ukoliko je heš zaglavlja bloka manji ili jednak od cilja heša [4]. Glavna motivacija čvorova da učestvuju u ovom procesu jeste nagrada koju dobije nakon dodavanja bloka u lanac.

BFT algoritmi se zasnivaju na komunikacionim protokolima u kojima čvorovi imaju jednake glasove i prolaze kroz više rundi komunikacija kako bi postigli konsenzus. Ova grupa algoritama se koristi kod privatnih tipova blokčejn mreže jer im odgovara manji broju učesnika u mreži i omogućavaju brže potvrđivanje transakcija. Glavni predstavnik je *Practical Byzantine Fault Tolerant* (PBFT) algoritam. Za ovaj algoritam je karakteristično to što ne dozvoljava da broj zlonamernih čvorova bude veći od 1/3 [4]. Ukoliko broj zlonamernih čvorova prelazi 1/3, konsenzus između čvorova se ne može postići.

2.4. Princip rada blokčejn tehnologije

Kreiranje i dodavanje novog bloka u lanac se postiže kroz sledeća 4 koraka [4]:

- Nastupanje transakcije – kad god čvor ima za cilj interakciju sa drugim čvorom iste mreže, nastupa nova transakcija (npr. transfer kriptovaltuta),
- Propagacija transakcije – kako se radi o P2P mreži, potrebno je da svaki čvor pošalje transakciju svojim susednim čvorovima. Ovaj postupak se ponavlja sve dok svi čvorovi mreže nemaju kod sebe podatke o transakciji,
- Validacija (bloka) transakcije – pre smeštanja transakcije u blok, potrebno je da se izvrši njena verifikacija od strane čvorova mreže. Verifikacija transakcije se odnosi na proveru ispravnosti njenog kriptografskog heša. Po uspešnoj proveri, transakcija dobija odobrenje da se doda u blok. Zatim, potrebno je da se nađe sporazum između čvorova o validnosti bloka tj. čvorovi se moraju složiti oko redosleda nastupanja transakcija i izračunate heš vrednosti bloka pomoću konsenzus protokola mreže,
- Potvrda (bloka) transakcije – potvrda bloka predstavlja njegovo uključenje u lanac blokčejna. Potvrda transakcije se javlja kada se većina čvorova mreže složi o potvrdi, a zatim objavi blok koji sadrži datu transakciju.

3. Poređenje blokčejn simulatora

Za poređenje uzeti su sledeći blokčejn simulatori: *BlockSim: Faria* (BSF) [6], *BlockSim: Alharby* (BSA) [7], *SIMBA* [8], *Zelig* [9], *SimBlock* (SB) [10], *VIBES* [11] i *eVIBES* [12].

3.1. Poređenje blokčejn simulatora prema njihovim karakteristikama

Tabela 1 prikazuje informacije vezane za karakteristike blokčejn simulatora, kao što su: koje blokčejn platforme simulira, koje slojeve analizira („K“ za sloj konsenzusa, „P“ za sloj podataka i „M“ za sloj mreže), tip modela, programski jezik, dostupnost izvornog koda simulatora („+“ znači da je dostupan, a „-“ znači da nije dostupan) i datum poslednje izmene koda simulatora.

Tabela 1. Pregled karakteristika izabranih blokčejn simulatora

Simulator	Platforme	Slojevi	Tip modela	Prog. jezik	Izvorni kod	Poslednja izmena
BSF	*Bitcoin*, *Ethereum*	K, P, M	Diskretan	*Python*	+	19.05.2020.
BSA	PoW blokčejn	K, P	Diskretan	*Python*	+	18.05.2021.
SIMBA	*Bitcoin*	K, P, M	Diskretan	*Python*	+	20.05.2020.
Zelig	*Bitcoin*	K, P, M	Diskretan	*Python*	+	24.08.2021.
SB	PoW blokčejn	K, M	Diskretan	*Java*	+	12.02.2021.
VIBES	PoW blokčejn	K, P	Diskretan	*Scala*	+	25.04.2020.
eVIBES	*Ethereum*	K, P	Diskretan	*Scala*	+	12.03.2019.

Blokčejn platforme koje koriste PoW protokol trenutno dominiraju tržištem, gde čine skoro 70% celokupnog tržišta [13]. U skladu sa tim, ne treba da iznenadi to što svi izabrani simulatori koriste PoW protokol i što je *Bitcoin* glavni fokus među simulatorima.

Zbog višeslojne arhitekture blokčejn mreža, obično se i arhitektura simulatora sastoji od nekoliko slojeva. Simulacioni modeli se koriste za implementaciju ponašanja različitih slojeva i njihovih interakcija. Međutim, neki od njih su veoma pojednostavljeni. Zbog toga se u koloni „Slojevi" prikazuju samo slojevi konsenzusa, podataka i mreže. Značajno je da samo tri simulatora (BSF, SIMBA i Zelig) simuliraju sva tri sloja.

Generalno, blokčejn simulatori obično praktikuju simulaciju diskretnih događaja u kojima se stanja menjaju u diskretnim trenucima u vremenu, što je i ovde slučaj. Glavni programski jezik je *Python* (4 simulatora), zatim *Scala* (2 simulatora) i na kraju *Java* (1 simulator). Izvorni kodovi za svaki od simulatora su javno dostupni na *GitHub*-u.

3.2. Poređenje blokčejn simulatora prema njihovim ulaznim i izlaznim parametrima

Za potrebe ovog poređenja, glavni kriterijumi su bili: dostupnost izvornog koda, sposobnost eksperimentisanja sa većim brojem funkcija simulirane blokčejn mreže i mogućnost ažuriranja ulaznih podataka i parametara tako da odražavaju trenutno stanje u blokčejn mrežama. Prateći ove kriterijume, izabrano je 4 od 7 simulatora koje će se u nastavku razmatrati, a to su: BSF, BSA, SB i VIBES.

Ulazni i izlazni parametri blokčejn simulatora su prikupljeni kombinovanjem teorijskog dela (publikacija simulatora) i praktičnog dela (izvorni kod simulatora). Prikupljeni podaci za simulatore su prikazani u okviru Tabele 2, gde „D“ znači da simulator sadrži određeni parametar i „N“ što govori suprotno.

Tabela 2. Ulazni i izlazni parametri izabranih blokčejn simulatora

Sloj	Parametar	BSF	BSA	SB	VIBES
Ulazni podaci					
Mreža	Raspodela veličine bloka / fiksno	N / D	N / D	N / D	N / D
	Raspodela veličine transakcije / fiksno	N / D	D / N	N / N	N / D
	Lokacijska raspodela čvorova	D	N	D	N
	Raspodela broja čvorova u okruženju po čvoru / fiksno	N / D	N / N	D / N	N / D
	Lokacijska raspodela *miner*-a	D	N	N	N
	Lokacijska raspodela propusnog opsega	D	N	D	N
	Raspodela vremena kašnjenja	D	N	D	N
	Mehanizmi propagacije informacija	D	N	D	N
Konsenzus	PoW protokol / drugi	D / N	D / N	D / D	D / N
	Raspodela intervala bloka / fiksno	N / D	N / D	N / D	N / D
	Raspodela *mining* snage *miner*-a	D	D	D	D
	Dinamičko prilagođavanje težine *mining*-a	N	N	N	N
	Raspodela troškova transakcije / fiksno	N / N	D / D	N / N	N / D
Podaci	Mogućnost generisanja transakcija	D	D	N	D
	UTXO model / model zasnovan na nalogu	N / N	N / N	N / N	N / N
Ukupan broj dostupnih ulaznih parametara		12	8	10	8
Izlazni podaci					
Mreža	Srednja veličina bloka	D	D	N	D
	Srednji broj čvorova u okruženju po čvoru (običan i *miner*)	N	N	N	N
	Srednje vreme propagacije bloka (kašnjenje)	D	N	D	N
	Srednje vreme propagacije transakcije (kašnjenje)	N	N	N	D
	Propusni opseg (t/s)	N	D	N	D
Konsenzus	Srednje vreme intervala bloka	N	N	D	D
	Ukupan broj generisanih blokova	D	D	D	N
	Broj dodatih blokova	D	D	N	N
	Broj odbačenih blokova (%)	N	D	D	D
Ukupan broj dostupnih izlaznih parametara		4	5	5	5
Ukupan broj dostupnih ulaznih i izlaznih parametara		16	13	15	13

Uzimajući u obzir sloj mreže, BSF ima najrazvijeniji simulacioni model od svih analiziranih blokčejn simulatora. BSF pruža najveći broj različitih ulaznih parametara i približno isti broj izlaznih parametara u odnosu na ostale simulatore. SB i BSF, za razliku od ostalih simulatora, mogu prikazati jako dobro mrežni sloj zbog lokacijske raspodele čvorova, lokacijske raspodele propusnog opsega, raspodele vremena kašnjenja i mehanizama za propagaciju informacija. Ipak, važno ograničenje SB simulatora je to što ne pravi razliku između običnog čvora i *miner*-a. VIBES i BSA simulatorima nedostaje mogućnost realnog simuliranja ponašanja mreže (npr. oba koriste fiksno vreme kašnjenja za propagaciju transakcija i blokova). Trenutno, BSF simulator je pogodan samo za simulacije koje podrazumevaju mali broj čvorova u mreži. U ostalim simulatorima, moguće je simulirati mreže sa velikim brojem čvorova. U skladu sa tim, VIBES može da vrši simulacije sa velikim brojem čvorova (preko 10 000). Nedostatak svih simulatora je to što oni uglavnom koriste fiksan broj čvorova, što ne odgovara stvarnosti kada su javne blokčejn platforme u pitanju.

Analizirajući parametre kroz sloj konsenzusa, većina simulatora se fokusira isključivo na PoW protokole, a samo SB ima sposobnost simulacije uprošćenog PoS protokola. Neki simulatori, poput BSA i SB, pretpostavljaju da su svi čvorovi u mreži dobronamerni. Kao posledica toga, oni se ne mogu koristiti za istraživanje strategija zlonamernog ponašanja čvorova u mreži. Nasuprot tome, VIBES simulator se može koristiti za testiranje sigurnosti i za istraživanje potencijalnih napada. Nažalost, nijedan od izabranih simulatora ne primenjuje dinamičko prilagođavanje težine *mining* procesa.

Što se tiče sloja podataka, simulatori BSF, BSA i VIBES podržavaju simulaciju (generisanje) transakcija. Međutim, ovaj proces je ograničen jer simulatori ne implementiraju UTXO (eng. *Unspent Transaction Output*) model, a ni model zasnovan na nalozima. Glavna ograničenje SB simulatora je to što izvršava simulaciju blokčejn platformi samo na nivou bloka tj. propagacija transakcija nije u fokusu.

Na kraju, ukupan broj dostupnih ulaznih i izlaznih parametara je izračunat za svaki od izabranih simulatora. Na prvom mestu je BSF simulator (16), zatim na drugom mestu SB simulator (15) i treće mesto dele BSA i VIBES simulatori (13). Rangiranje simulatora ne znači da je neki bolji ili lošiji od drugog jer sve zavisi od toga šta je potrebno simulirati i u kojoj meri. Ne postoji univerzalni simulator koji bi se mogao primeniti na širok spektar različitih scenarija i problema. Mogućnosti postojećih simulatora su ograničene jer su dizajnirane da simuliraju neke od kritičnih scenarija i problema realnih blokčejn mreža, a ostale prikazuju u pojednostavljenom obliku.

4. Javna prodaja sadržine neisporučivih poštanskih pošiljaka putem blokčejna

Ovo poglavlje će biti podeljeno na dva dela. U prvom delu biće opisane neisporučive poštanske pošiljke i proces javne prodaje od strane Pošte, dok će u drugom delu biti prikazan i testiran proces javne prodaje u formi pametnog ugovora.

4.1. Javna prodaja sadržine neisporučivih poštanskih pošiljaka

Neisporučiva poštanska pošiljka je pošiljka za koju se utvrdi da se ne može uručiti ni primaocu, niti vratiti pošiljaocu, u rokovima predviđenim aktom JP Pošte Srbije kojim se uređuju posebni uslovi za obavljanje poštanskih usluga [14]. Rešenjem direktora radne jedinice obrazuje se komisija za pregled i rešavanje statusa sadržine neisporučivih

pošiljaka. Njeni zadaci su preuzimanje, pregled i otvaranje neisporučivih pošiljaka radi utvrđivanja adrese primaoca ili pošiljaoca, kao i organizovanje javne prodaje, neposredne pogodbe, ustupanja sadržine u humanitarne svrhe i komisijsko uništenje sadržine neisporučivih pošiljaka. U pogledu javne prodaje, zadaci komisije su da [14]:

- Proceni vrednost sadržaja pošiljke ili njenog dela i utvrdi početnu cenu za prodaju,
- Odredi i objavi mesto i vreme javne prodaje i postavi obaveštenje o tome u poslovnim prostorijama JP Pošte Srbije, kao i na Internet strani Pošte,
- Organizuje postupak javne prodaje (izloži robu, ispiše šifre artikala i početne cene, obezbedi fiskalnu kasu, i dr.),
- Sačini zapisnik o javnoj prodaji sadržine pošiljke ili njenog dela u koji se obavezno unosi početna i prodajna cena, a potpisuju ga članovi komisije i kupci,
- Po završenoj prodaji popisuje preostalu neprodatu robu i o tome sačini zapisnik u kome predlaže ustupanja sadržine pošiljaka u humanitarne svrhe.

Oglas o javnoj prodaji treba da sadrži: uslove javne prodaje, podatke o vrsti i stanju robe, početnu cenu robe, dan, čas i mesto održavanja javne prodaje. U Tabeli 3 je formirano 10 artikala koji će služiti kasnije za testiranje pametnog ugovora.

Tabela 3. Prvih 10 artikala javnog oglasa o prodaji sadržine neisporučivih pošiljaka

Red. br.	Vrsta robe	Stanje robe	Početna cena (din)
1	NARUKVICA-BIŽUTERIJA	POLOVNO	50.00
2	BLUZA	POLOVNO	50.00
3	SLUŠALICE 4 KOM	POLOVNO	50.00
4	SLUŠALICE 20 KOM	POLOVNO	100.00
5	PRSTEN-BIŽUTERIJA	POLOVNO	50.00
6	MINĐUŠE I NARUKVICA	POLOVNO	50.00
7	DUKS	POLOVNO	100.00
8	MINĐUŠE DVA PARA	POLOVNO	50.00
9	MINĐUŠE 2 PARA	POLOVNO	50.00
10	MAJICA-HALJINA	POLOVNO	50.00

Novčana sredstva dobijena prodajom sadržine pošiljke uplaćuju se na tekući račun radne jedinice i čuvaju godinu dana od isteka roka za čuvanje pošiljke. U istom roku se na tekućem računu radne jedinice čuva i novac pronađen u pošiljkama. Ako pošiljalac ne podnese zahtev za isplatu u roku od godinu dana od isteka roka za čuvanje te pošiljke, novčana sredstva od prodaje sadržine neisporučive pošiljke, kao i novčana sredstva pronađena u pošiljkama, postaju vanredni prihod JP Pošte Srbije.

Sadržina neisporučivih pošiljaka koje u postupku javne prodaje ili neposredne pogodbe nisu prodate, ustupaju se bez naknade trećim licima u humanitarne svrhe. Sadržina pošiljaka koja nije prodata javnom prodajom, neposrednom pogodbom ili ustupljena u humanitarne svrhe, komisijski se uništava.

4.2. Realizacija pametnog ugovora javne prodaje sadržine neisporučivih poštanskih pošiljaka

Za potrebe realizacije javne prodaje (aukcije) u formi pametnog ugovora na *Ethereum* blokčejnu, korišćeni su programski jezik *Solidity*, razvojno okruženje *Remix*, lokalni blokčejn *Ganache* i novčanik za kriptovalute *MetaMask*. Kod pametnog ugovora se nalazi na *GitHub* platformi [15]. Nakon svih potrebnih podešavanja (stvaranje korisničkih naloga, formiranje lokalne blokčejn mreže, itd.) i međusobnog povezivanja programa, moguće je pokrenuti pametan ugovor i realizovati test primer javne prodaje.

Vlasnikom pametnog ugovora se smatra javna adresa blokčejn mreže koja ga je pokrenula, u ovom test primeru je to Pošta. Pošta jedina ima sposobnost da unese artikle koji su namenjeni za javnu prodaju, da postavi njihove početne cene i opis, da definiše vreme početka i kraja javne prodaje, itd. Artikli iz Tabele 3 biće uneti i korišćeni za potrebe ovog test primera. Radi boljeg pregleda promena u mreži uvodi se pretpostavka da je 1 ETH jednak 1 dinar i da je vreme trajanja javne prodaje deset minuta. U okviru programa *Ganache*, generisani su korisnički nalozi koji će se koristiti u ovom test primeru. Tabelom 4 prikazani su svi korisnički nalozi od kojih je prvi nalog (indeks 0) rezervisan za Poštu.

Tabela 4. Indeks, javna adresa i početni balans korisničkih naloga

Indeks	Javni ključ (javna adresa)	Balans (ETH)
0	0x5887a454080e4f3BFceCe6d85e8d9a7c1D6Cb5f5	500.00
1	0x23bB2F4aa7B3B25127129290278DaB590bF8E21D	500.00
2	0xF34814Dd409e460591BD0497A55F3f6fE61EdF95	500.00
3	0x49CaaE5B6c53B207726731D5Da3C48b3B6Cf7f45	500.00
4	0x0Fb90faa0d06FC79646D42132571D6f066973955	500.00
5	0x0DB07F2e9C69B88164dB3283d82112B79EE0878f	500.00
6	0x16C5cB04b8decF69958bE63d5A8CF50c260d1816	500.00
7	0xa4848A1cd36B35421FCa1bCC0AC24796b5F055Ac	500.00
8	0x6918f488b6D6b619628e33e3847CFc02Eb641f6c	500.00
9	0x7e14Caebae7954227fc35457D33ad5BD2484e53C	500.00

U lokalnoj blokčejn mreži potrebno je preuzeti kontrolu nad korisničkim nalozima i izvršiti licitaciju. Po isteku vremena za trajanje aukcije Pošta objavljuje njen kraj. Korisnici sa pobedničkim licitacijama mogu preuzeti vlasništvo nad artiklima. Korisnici koji nisu imali pobedničke licitacije mogu povući svoje iznose licitacija. Tabela 5 daje balanse korisničkih naloga nakon završetka aukcije, kao i nove vlasnike artikala.

Tabela 5. Pregled stanja nakon završene aukcije

Indeks korisnika	Red. br. artikla kojih je vlasnik nakon aukcije	Pobednička licitacija (ETH)	Balans nakon aukcije (ETH)
0	10	/	1669.92
1	4	280.00	220.00
2	3	120.00	379.99
3	/	/	499.99
4	7	220.00	280.00
5	/	/	500.00
6	/	/	500.00
7	2	80.00	419.99
8	1, 5	100.00, 100.00	299.99
9	6, 8, 9	70.00, 100.00, 100.00	229.98

Artikli koji nisu imali nijednu licitaciju tokom trajanja aukcije, ostaju u vlasništvu Pošte (artikal sa rednim brojem 10). Ovim se kompletno završava proces obavljanja javne prodaje sadržaja neisporučivih poštanskih pošiljaka.

5. Zaključak

Blokčejn ima potencijal da utiče na sektore koji se oslanjaju na posrednike. Postaje jako aktuelna za izučavanje, testiranje i pokušaje implementacije. Budući da će izazvati promene u oblastima poslovanja raznih industrija, praćenje razvoja i početak eksperimentisanja moglo bi koristiti preduzetnicima kao i njihovim korisnicima.

Svaki od 7 blokčejn simulatora ima neke svoje funkcionalnosti, ali i dosta sličnosti sa ostalim simulatorima. Zbog toga, ovi simulatori su se koristili za međusobno poređenje, analizu i dolaženje do novih saznanja. Poređenjem prema njihovim karakteristikama, dolazi se do saznanja da simulatori u najvećoj meri izvršavaju simulaciju PoW blokčejn platformi, koriste *Python* programski jezik i koriste simulaciju diskretnih događaja. Zatim, ukoliko se porede prema njihovim ulaznim i izlaznim parametrima, dolazi se do saznanja da *BlockSim: Alharby* daje najviše mogućnosti (ukupno 16 dostupnih parametara). Takođe, na primeru odvijanja procesa javne prodaje sadržine neisporučivih poštanskih pošiljaka, korišćenjem pametnog ugovora za aukciju, može se videti jedna od primena blokčejn tehnologije čime se podstiče automatizacija procesa u poštanskoj industriji.

Literatura

[1] S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System", 2008. [Online]. Available at: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, "A next-generation smart contract and decentralized application platform", 2014. [Online]. Available at: https://ethereum.org/en/whitepaper/.

[3] T. T. A. Dinh, R. Liu, M. Zhang, and G. Chen, "Untangling Blockchain: A Data Processing View of Blockchain Systems", *IEEE Transactions on Knowledge & Data Engineering*, vol. 30, pp. 1366-1385, 2018. DOI: 10.1109/TKDE.2017.2781227.

[4] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How", *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 3796-3838, 2019. DOI: 10.1109/COMST.2019.2928178.

[5] W. Zheng et al., "NutBaaS: A Blockchain-as-a-Service Platform", *IEEE Access*, vol. 7, pp. 134422-134433, 2019. DOI: 10.1109/ACCESS.2019.2941905.

[6] C. Faria and M. Correia, "BlockSim: Blockchain Simulator", *2019 IEEE International Conference on Blockchain*, pp. 439-446, 2019. DOI: 10.1109/Blockchain.2019.00067.

[7] M. Alharby and A. Moorsel, "BlockSim: An Extensible Simulation Tool for Blockchain Systems", *Frontiers in Blockchain*, vol. 3, 2020. DOI: 10.3389/fbloc.2020.00028.

[8] S. M. Fattahi, A. Makanju, and A. Milani Fard, "SIMBA: An Efficient Simulator for Blockchain Applications", *2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*, pp. 51-52, 2020. DOI: 10.1109/DSN-S50200.2020.00028.

[9] E. Erdogan et al., "Zelig: Customizable Blockchain Simulator", 2021.

[10] Y. Aoki et al., "SimBlock: A Blockchain Network Simulator", *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 325-329, 2019. DOI: 10.1109/INFCOMW.2019.8845253.
[11] L. Stoykov, K. Zhang, and H. Jacobsen, "VIBES: fast blockchain simulations for large-scale peer-to-peer networks", *Proceedings of the 18th International Middleware Conference*, 2017. DOI: 10.1145/3155016.3155020.
[12] A. Deshpande, P. Nasirifard, and H. Jacobsen, "eVIBES: Configurable and Interactive Ethereum Blockchain Simulation Framework", *Proceedings of the 19th International Middleware Conference*, 2018. DOI: 10.1145/3284014.3284020.
[13] Cryptoslate. [Online]. Available at: https://cryptoslate.com/cryptos/proof-of-work/.
[14] *Službeni PTT Glasnik*, broj 935, 2014.
[15] Projekat na *GitHub*-u. [Online]. Available at: https://github.com/nikola97m/aukcija-pametan-ugovor/blob/main/solidity.

Abstract: *Although various solutions based on blockchain technology have been created, the lack of tools to evaluate these complex distributed systems can hinder the development and progress of this area. Exploring different implementations and different design variations of blockchain technology is complicated and difficult to perform on real systems. Meanwhile, blockchain simulators provide the ability to display real processes at a low cost. Simulators can test performance using different settings and parameters on a single computer. This paper provides an analysis of 7 blockchain simulators and their comparison. Also, blockchain technology was used for the realization of the process of public sale (auction) of the contents of undeliverable postal items. This process is realized on the blockchain using smart contracts.*

Keywords: *blockchain, Bitcoin, blockchain simulator, smart contract, public sale.*

BLOKCHAIN – SIMULATION TESTING OF NETWORK AND AN IMPLEMENTATION OF AUCTION SALE SMART CONTRACT

Nikola Matijašević, Marko Đogatović